CONTACT: Mary Jane Collipriest (Bennett) 202-224-5444
Bill Ghent (Carper) 202-224-8395

FOR IMMEDIATE RELEASE

June 26, 2006

BENNETT, CARPER INTRODUCE SECURITY BREACH LEGISLATION

Bill Safeguards Sensitive Consumer Information, Helps Prevent Identity Theft

WASHINGTON, DC – Sen. Bob Bennett (R-Utah) and Sen. Tom Carper (D-DE), members of the Senate Banking Committee, today introduced legislation to help protect individuals and businesses from the rampant crimes of identity theft and account fraud.

"The conveniences and efficiencies of the Information Age, which have brought economic benefits and improved quality of life, have also brought new challenges," said Sen. Bennett, chairman of the Senate Banking Subcommittee on Financial Institutions. "Thieves, cheats and other criminals have also entered the Information Age, and are using information technology to steal from many of us. Too many Americans have become victims of identity theft or account fraud, and these crimes are increasing at an alarming rate.

"Though current law requires financial institutions to protect the security and confidentiality of customer information, we have to expand this reach. Many of the recent breaches in data security have occurred outside financial institutions' networks," Bennett added. "We are not doing enough to protect consumers and businesses from identity theft and account fraud as criminals have shown they can exploit any network weakness, regardless of where they are located. The bill I'm introducing with Senator Carper goes a long way to fill these holes in the system."

Senator Carper said, "We used to just worry about people breaking into our homes or stealing our cars, but in the 21st century, we have to worry about people stealing our identities via computers and the Internet. Given what we've seen happen recently with the security lapses at the Veterans Administration and other financial institutions, it's imperative that we write a national law to help protect consumers from being victims of identity theft. This bill would require all financial institutions, retailers and government

agencies to maintain strong internal safety protections for the data they hold, to quickly investigate any security breach, and notify law enforcement, regulators and the public when there's a real risk of harm."

The Data Security Act of 2006 is modeled after the data security and security breach response regime established under the Gramm-Leach-Bliley Act of 1999 (GLB) and subsequent regulations. The new bill requires that all entities, not just financial institutions, safeguard sensitive information and notify consumers when information is breached in a way that could lead to identity theft or account fraud.

The Bennett-Carper legislation creates a uniform national standard to safeguard sensitive information and provide consumer notification of security breaches. It also models enforcement provisions after the GLB blueprint so federal and state regulators who oversee financial institutions, and other entities that have this information, are equipped with the tools to enforce these protections against data security breaches and help consumers mitigate the problems that result.

Key points of The Data Security Act of 2006 follow:

Creates a Uniform National Standard

Today, more than 30 states have enacted security breach notification laws and several others may pass laws this year. Though some are similar, many have inconsistent and conflicting standards which present significant challenges in protecting consumers' sensitive information and notifying consumers whose security has been breached. Differing state laws result in higher costs and uneven consumer protection.

Under the Bennett-Carper bill, all entities that handle sensitive information will be subject to a uniform national standard for data protection and breach notification that will be implemented and enforced by the regulator that knows them best.

"A national patchwork of inconsistent laws leads to confusion, delays and higher costs," said Bennett. "It makes it more difficult to notify consumers in a timely manner, particularly when they need to act quickly to protect themselves. We need a national standard to ensure that all consumers are equally protected, regardless of where they live."

Includes Risk-based Trigger for Consumer Notification of Data Breach

The Data Security Act ensures that consumers will be notified when their sensitive information is lost or stolen and may lead to harm. Modeled after GLB law and regulations, it requires all entities to investigate possible breaches and inform their regulators when sensitive consumer information may have been lost. This bill uniformly applies the GLB's statutory standard of "substantial harm or inconvenience" to all entities that maintain, communicate or posses sensitive

personal or account information. "Substantial harm or inconvenience" includes identity theft or account fraud situations where consumers experience financial loss or are forced to expend significant time and effort to correct false information.

Broad consumer notice would not be required if the information lost or stolen is not useable to commit fraud, through encryption, for example through, or other technology.

Ensures State and Federal Functional Regulators Have Right to Enforce Requirements of Data Security Breach

The Data Security Act of 2006 provides that federal and state regulators of banks, thrifts, credit unions, securities brokers and insurance companies will continue to have the right to enforce requirements of data breach and notification. Other types of entities will fall within the enforcement jurisdiction of the Federal Trade Commission (FTC).

The bill will be referred to the Senate Banking Committee where it will be the subject of hearings.

For a copy of the bill summary, opening statements by Senators Bennett and Carper, as well FAQs of the measure, please go to the senators' websites at http://bennett.senate.gov or http://carper.senate.gov

#####